VA Secure Design Review Introduction

- About Secure Design Review / Application Threat Modeling
- VA Secure Design Review Authorization Requirement
- VA Secure Design Review Standard Operating Procedures
- VA Secure Design Review Workflow
- Additional Slides VA Secure Design Review Resources
- Additional Slides VA Secure Design Review Example

About VA Secure Design Review / Application Threat Modeling

- Broadly speaking, application-level vulnerabilities manifest themselves as one of two types:
  - Design flaws introduced by weaknesses during the requirements, design, or architecture phase; or
  - Implementation bugs introduced by weaknesses during the actual coding of the application.
- Secure design reviews of VA custom-developed applications are now intended to be conducted during development and also during authorization processes.
- Secure design reviews unlike secure code reviews may be (and are recommended to be) performed before any code is written.

VA Secure Design Review Authorization Requirement

- Accreditation Requirements Guide SOP Security Documentation Requirements Section “Secure Design Review”
  - Secure Design Review (Application Threat Modeling) guidance
  - Secure Design Review completion steps
  - Continuous Monitoring Requirement
- Requirements reference:
  - VA Secure Design Review Standard Operating Procedures
  - VA Software Assurance Developer Support Site

VA Secure Design Review Standard Operating Procedures

- VA Secure Design Review Standard Operating Procedures (SOP)
  - While VA Secure Code Review SOP focuses primarily upon implementation bugs, VA Secure Design Review SOP focuses on design flaws.
  - This SOP leverages the Microsoft Threat Modeling Tool that supports the “Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege” (STRIDE) threat modeling process. STRIDE is an iterative process where an application’s design is systematically decomposed and formulaically analyzed for vulnerabilities.

VA Secure Design Review Workflow

1. If it has not been done already, register the application with VA SwA Program Office
2. Upload required lists of technologies/libraries utilized, sequence diagrams, and other requested information to the VA SwA file server
3. Open a NSD ticket according to VA SwA Program Office procedures to request the development of an initial threat model diagram
4. Work iteratively with VA SwA Program Office to develop an initial threat model diagram based on the initial documentation provided
5. Analyze the collaboratively-developed model to determine appropriate mitigations to identified potential vulnerabilities
6. Upload finalized threat model file, documentation supporting threat model mitigations, and other requested information
7. Open a NSD ticket according to VA SwA Program Office procedures to request the validation of the finalized threat model diagram

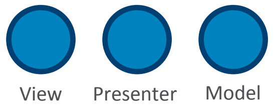
Additional Slides VA Secure Design Review Resources

- VA Secure Design Review SOP https://wiki.mobilehealth.va.gov/download/attachments/24482308/VA%20Secure%20Design%20Review%20SOP.pdf?api=v2
- VA Software Assurance Support Site https://wiki.mobilehealth.va.gov/display/OISSWA
- VA Software Assurance Support Site Secure Design Review Service Request Procedures & Forms https://wiki.mobilehealth.va.gov/display/OISSWA/Frequently+Asked+Questions
- VA Software Assurance Support Site Secure Design Review Technical Notes https://wiki.mobilehealth.va.gov/display/OISSWA/7.+Microsoft+Threat+Modeling+Tool

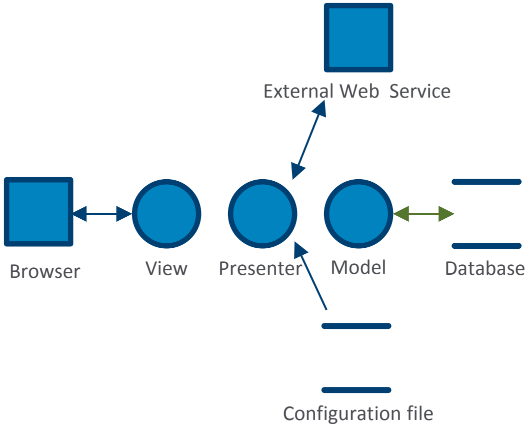
Additional Slides VA Secure Design Review

- Notional example:

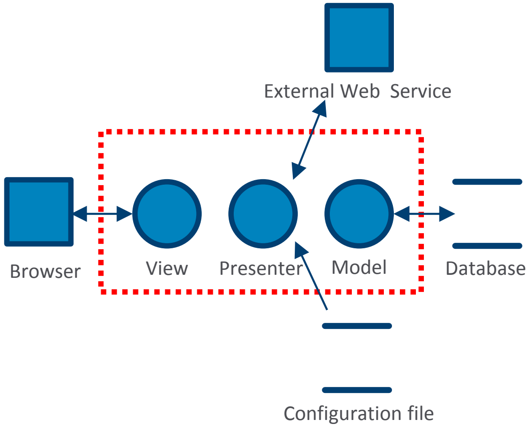
Step 1. Start With A Design Pattern



Step 2. Add Architectural Elements



Step 3. Add Trust Boundaries


External Web Service
Browser
View
Presenter
Model
Database
Configuration file